Isoranta Olli

SIMULAATIO-OPPIMISYMPÄRISTÖN TIETOTURVAKARTOITUS

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikan ja liikenteen ala
Tietoturvan koulutusohjelma
Syksy 2012

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikka ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Isoranta Olli	
Työn nimi Simulaatio-oppimisympäristön tietoturvakartoitus	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Raili Simanainen
	Toimeksiantaja Kajaanin ammattikorkeakoulu Sairaan- ja terveydenhoito-osaamisalue / Jaana K.
Aika Syksy 2012	Sivumäärä ja liitteet 30+1

Tämän opinnäytetyön tavoitteena oli tehdä tietoturvakartoitus Kainuun ammattiopiston ja Kajaanin ammattikorkeakoulun simulaatio-oppimisympäristölle.

Simulaatio-oppimisympäristö hankittiin vuoden 2011 lopussa, ja sen tavoite on parantaa käytännön osaamista, tilannetietoisuutta, kommunikaatiota sekä ei-teknisiä taitoja, kuten tiimityöskentelyä sairaan- ja terveydenhoito-osaamisalueilla. Simulaatio-oppimisympäristöjen etu tavalliseen opetukseen verrattuna on teoriataitojen testaaminen käytännössä sekä virheiden analysointi ja niistä oppiminen.

Opinnäytetyön alussa tutustutaan simulaatio-opetukseen, jota käytetään muun muassa lääketieteenaloilla sekä teollisuuden aloilla. Opinnäytetyössä tutustutaan myös tarkemmin Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston simulaatio-oppimisympäristöön. Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston simulaatio-oppimisympäristö on fyysinen, joka hyödyntää tietotekniikkaa. Insinöörityön teoriaosuudessa on tutustuttu tietoturvan peruskäsitteisiin, osa-alueisiin sekä riskianalyysimenetelmiin, kuten tarkistuslistoihin, SWOT-analyysiin ja väärinkäyttöskenaariohin, jotta tietoturvakartoituksen tarkoitus olisi helpompi ymmärtää. Insinöörityön käytännön osuus sisältää tietoturvakartoituksen Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston simulaatio-oppimisympäristöstä. Tietoturvakartoitus toteutettiin haastattelemalla ympäristöä käyttäviä henkilöitä sekä osallistumalla opetustilanteeseen työtapojen ja käytäntöjen seuraamiseksi. Haastattelujen aikana henkilöiltä kysyttiin teoriaosuuteen pohjautuvia kysymyksiä, joiden tarkoitus oli ohjata keskustelua sekä paljastaa mahdollisia tietoturva-aukkoja.

Tietoturvakartoituksen tuloksena saatiin selville simulaatio-oppimisympäristön tietoturvan nykytilanne. Tietoturvakartoituksen aikana ilmeni muutamia tietoturva-aukkoja sekä puutteellisuuksia, joihin esitettiin kehittämisehdotuksia. Tietoturva-aukkoihin puututtiin nopeasti ja kehitysehdotukset otettiin käyttöön jo työn aikana. Simulaatio-oppimisympäristön tietoturva-aukkoja tai asiakkaalle esitettyjä kehitysehdotuksia ei ole insinöörityöhön lisätty, insinöörityön luonteen vuoksi.

Kieli	Suomi
Asiasanat	Tietoturva, Tietoturvakartoitus, Simulaatio-oppimisympäristö
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Isoranta Olli	
Title Assessing the Information Technology Security of a Simulation Environment	
Optional Professional Studies Information Security Technology	Instructor(s) Ms Raili Simanainen
	Commissioned by Kajaani University of Applied Sciences Ms Jaana Kemppainen
Date Fall 2012	Total Number of Pages and Appendices 30+1

The purpose of this Bachelor's thesis was to examine the level of information security at the simulation environment of the Kajaani University of the Applied Sciences and Kainuu Vocational College. The simulation environment was taken to use at the end of the year 2011.

The purpose of the simulation environment is to improve situation awareness, performance in practice, communication and non-technical skills such as teamwork in healthcare environments. When compared to theoretical teaching, the advantage of simulation environment teaching is the possibility to test theoretical skills in practice as well as to analyze mistakes and learn from them.

The beginning of the thesis introduces different kinds of simulation environments. It also introduces the simulation environment of the Kajaani University of Applied Sciences and Kainuu Vocational College in more detail. The theoretical part of the thesis introduces terms, concepts and risk assessment methods connected with information technology security in order to make the practical part of the thesis easier to understand.

The practical part of the thesis focuses on the risk assessment of the simulation environment. The risk assessment was carried out by interviewing personnel using the environment and observing lessons in order to get more information about people's behavior.

During the interviews, the personnel were asked questions based on the theoretical part of the thesis. The purpose of these questions was to reveal potential weaknesses in information technology. A couple of weaknesses were located, and suggestions how to improve them were given. The weaknesses and improvement suggestions are not listed in this thesis because of the nature of the thesis.

Language of Thesis	Finnish
Keywords	Information Security, Data Security, Information Technology Security Assessment, Risk Assessment, Simulation Environment
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

ALKUSANAT

Kiitos Raili Simanaiselle, hyvästä ohjauksesta työn aikana sekä myös Jukka Heinolle, joka antoi muutamia vinkkejä insinöörityön alkuaikoina. Kiitos myös Eero Soiniselle kieliasun ohjauksesta.

Kiitokset myös Taina Romppaselle, Jukka Seppäselle sekä Jari Juntuselle, jotka osallistuivat riskienkartoitushaastatteluihin ja omasivat hyvän asenteen tietoturvaa kohtaan.

Kiitos myös TTI9K-luokkalaisille, jotka kannustivat ja innostivat insinöörityön aikana. Kiitokset kuuluvat myös fysioterapeutilleni, Jukka Nevalaiselle, joka helpotti työn tekemistä viikoittaisten fysioterapiakäyntien kautta.

SISÄLLYS

TERMILUETTELO

Autentikointi	Prosessi, jossa varmistetaan henkilön henkilöllisyys erilaisten menetelmien avulla.
Briefing	Keskustelu, jossa molemmille osapuolille annetaan toimintaohjeet ja heidät tuodaan ajan tasalle.
Bugi	Ohjelmistovirhe.
Debriefing	Keskustelu, jossa molemmat osapuolet analysoivat suoritettua toimintaa.
Debuggaus	Prosessi, jonka aikana paikannetaan virheitä erilaisten menetelmien avulla.
Kryptaus	Prosessi, jonka aikana salataan tietoa.
Riski	Mahdollinen negatiivinen poikkeama tavoitteesta.
Sertifikaatti	Sähköinen todistus, joka sisältää joukon tietoa, jonka sertifikaatin myöntäjä on tarkistanut ja todennut oikeiksi. Tunnetaan myös nimellä varmenne.
Simulaatio	Tilanne, jossa turvallisessa ympäristössä harjoitellaan tiettyä toimintaa keksittyjen tapausten avulla.
Skenaario	Tietyn tilanteen yksi tapaus.
Tietoturva	Pyrkii säilyttämään kerätyt tiedot eheinä, luottamuksellisina ja saatavilla. Kohteena voi olla esimerkiksi taloudelliset tiedot. [1.]
Virus	Haittaohjelma, joka saastuttaa koneen.

1 JOHDANTO

Kajaanin ammattikorkeakoulu on yhteistyössä Kainuun ammattiopiston kanssa hankkinut vuoden 2011 lopussa simulaatio-oppimisympäristön, jota käytetään erilaisten hoitoskenaarioiden harjoitteluun sairaan- ja terveydenhoidon osaamisalueella. Simulaatio-oppimisympäristön tarkoitus on kehittää osallistujien ei-teknisiä taitoja, kuten tiimityötä, tilannetietoisuutta ja kommunikaatiota. Simulaatio-oppimisympäristöä käytetään joka arkipäivä. Kajaanin ammattikorkeakoulu ja Kainuun ammattiopisto ylläpitävät simulaatio-oppimisympäristöä yhteistyöllä, ja ne ovat todenneet simulaatio-opetuksen hyväksi ja toimivaksi opetusmenetelmäksi. [2.]

Tietoturvalla pyritään suojelemaan yksityisten henkilöiden tai organisaatioiden arkaluontoisia sekä tärkeitä tietoja, jotka voivat aiheuttaa vahinkoa henkilöille tai organisaatiolle. Tietoturvatietoisuuden lisäämiselle on selvä tarve, sillä tietoturvavahingoissa on toistuvasti ollut kyse siitä, ettei uhkaa ole käytännön tilanteessa tiedostettu, oikeita menettelyjä ei ole tiedetty tai ohjeita ei ole noudatettu [3]. Tekniset ratkaisut eivät pysty ennustamaan käyttäjien toimintoja, jonka vuoksi henkilöt ovat tietoturvan tärkeimpiä tekijöitä [3]. Henkilöstön koulutus on avainasemassa tietoturvatietoisuuden lisäämisessä [3]. On myös hyvä muistaa, että jokainen on omalta osaltaan vastuussa tietoturvallisuudesta ja jokainen vaikuttaa sen toteutumiseen [3]. Jokaisella henkilöllä on jotakin tietoa, mitä hän ei halua muille paljastaa. Suojattavan tiedon määrä ja laatu on kuitenkin yksilöllistä.

Tämän insinöörityön tavoitteena on tehdä Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston simulaatio-oppimisympäristölle tietoturvakartoitus. Tietoturvakartoituksen tarkoitus on löytää ympäristöä uhkaavia tekijöitä, sen haavoittuvuuksia ja heikkouksia sekä pyrkiä estämään, ehkäisemään ja minimoimaan niitä. Tietoturvakartoituksen aikana simulaatio-oppimisympäristön ylläpitäjille ehdotetaan kehitysideoita ympäristön tietoturvan kehittämiseksi. Työn toimeksiantajana toimi Kajaanin ammattikorkeakoulun sairaan- ja terveydenhoito-osaamisalueen tuntiopettaja, Jaana Kemppainen.

2 SIMULAATIOJÄRJESTELMÄT OPETUKSESSA

Simulaatioympäristöt pyrkivät jäljittelemään todellisia tilanteita turvallisessa ympäristössä. Simulaatioympäristön etuna on harvinaisten tilanteiden harjoittelu, käytännön osaamisen parantuminen, virheiden salliminen, analysointi ja niistä oppiminen. Simulaatio-opetusta käytetään muun muassa aloilla, joissa henkilön tekemät virheet voivat johtaa ihmishenkien menetykseen. Näitä aloja ovat muun muassa useat lääketieteen alat, lentoala, merenkulun ala sekä useat teollisuudenalat, kuten esimerkiksi ydinvoimateollisuus. Myös armeija käyttää simulaatio-opetusta hyödyksi erilaisten taisteluskenaarioiden harjoitteluun. [4.]

Simulaatio-opetusta voidaan käyttää myös organisaation, työyhteisön tai -ryhmän toiminnan arvioimiseen, sillä simulaatiotilanteissa osallistujilta vaaditaan sekä teorian tuntemista että käytännön osaamista. Simulaatio-opetuksella pyritäänkin kokonaisvaltaiseen oppimiseen, sillä pelkän teorian osaamisesta ei ole hyötyä, jos sitä ei osata soveltaa käytännössä. [2.]

Simulaatiotilanteessa osallistujat toimivat käytännössä ja reagoivat tilanteisiin niin kuin he tekisivät oikeassa tilanteessakin. Osallistujat joko valitsevat oman roolinsa tai ohjaajat ovat ennalta määritelleet jokaisen osallistujan roolin. Jokainen osallistuja toimii oman roolinsa mukaisesti ja reagoi tilanteeseen roolinsa kautta. Toimintaosuuden jälkeen osallistujat analysoivat heidän tekemiään päätöksiä toimintaosuuden aikana ohjaajien kanssa. Analysoinnin tarkoitus on ymmärtää mikä johti osallistujan päätökseen ja mitä vaikutuksia päätöksellä oli, sillä pelkkä tilanteen kokeminen ja oikeiden vastausten kuuleminen ei takaa oppimista. [2.]

Simulaatioympäristöt voidaan karkeasti jakaa kolmeen ryhmään: virtuaaliset, fyysiset sekä niiden yhdistelmät. Virtuaaliset simulaatioympäristöt ovat pelkästään ohjelmistoja, joita voidaan käyttää tietokoneen avulla. Ohjelmistoon syötetään kaikki tarvittavat tiedot, kuten haluttu tilanne ja kappaleiden mitat. Tämän jälkeen ohjelmisto suorittaa tilanteen annetuilla arvoilla ja ilmoittaa tuloksen. Esimerkiksi tuloksena voi olla, että kappaletta ei voida kääntää tietyssä tilassa. Kehittyneimmät simulaatio-ohjelmistot yleensä simuloivat tilannetta reaaliajassa ja havainnollistavat sitä kuvalla. Virtuaalisia simulaatioympäristöjä käytetään yleensä teollisuudenaloilla.

Fyysiset simulaatioympäristöt on rakennettu johonkin tiettyyn tilaan, ja ne voivat hyödyntää tietokonejärjestelmiä. Fyysisiä simulaatioympäristöjä käytetään yleensä sosiaali- ja terveyspal-

velualoilla esimerkiksi ensihoitotilanteiden harjoitteluun. Henkilöille, jotka eivät työskentele sairaan- ja terveydenhoitoaloilla, tutuin ensihoitotilanne on todennäköisesti elvytys. Yksinkertaisin fyysinen simulaatioympäristö elvytystilanteesta voidaan toteuttaa elvytettävän nuken avulla, mutta yleensä fyysiset simulaatioympäristöt tekevät tilanteesta monimutkaisemman. Esimerkiksi nuken arvoja voidaan muuttaa tietokonejärjestelmän avulla ja joitain osallistujia on voitu ohjeistaa toimimaan elvyttäjää vastaan tai auttamaan häntä. Näillä muutoksilla simuloituun tilanteeseen saadaan mukaan oikean elämän häiriötekijöitä sekä muuttujia, joiden avulla tilanne saadaan tuntumaan oikealta.

Simulaatiojärjestelmä, joka toteutetaan sekä fyysisen että virtuaalisen simulaatiojärjestelmän avulla, on esimerkiksi lentäjien kouluttamiseen käytettävä lentosimulaatiojärjestelmä. Järjestelmä sisältää sekä ohjelmiston että fyysisiä komponentteja. Fyysisten komponenttien avulla voidaan simuloida lentäjän ohjaamoa, ja ohjelmiston avulla voidaan simuloida haluttua tilannetta. Esimerkiksi tilanteena voi olla lentokoneella laskeutuminen. Simulaatiossa käyttäjä ohjaa virtuaalista lentokonetta käyttämällä fyysisiä komponentteja ohjelmiston ohjaamiseen.

Simulaatio-opetus on havaittu hyväksi ja toimivaksi tekniikaksi, sillä ympäristössä voidaan kouluttaa uusia henkilöitä ja kokeneet henkilöt pystyvät kertaamaan hankalia sekä harvinaisia tilanteita. Opetus on myös mielenkiintoista osallistujien kannalta, koska he pystyvät oppimaan käytännön kautta. Sairaan- ja terveydenhoito-osaamisalueilla simulaatio-opetuksen on huomattu lisäävän potilasturvallisuutta, yhteistyötaitoja sekä päätöksentekokykyä. [2.]

3 TIETOTURVAN PERUSPERIAATTEET JA OSA-ALUEET

Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen suojaamista. Suojauksen tarkoitus on esimerkiksi estää luvattomilta käyttäjiltä pääsy tietoihin sekä suojata tieto olosuhteiden aiheuttamilta riskeiltä, kuten esimerkiksi vesivahingoilta. Suojaukselle on annettu yleinen käsite tietoturva, joka on jaoteltu useisiin käsitteisiin sekä asiakokonaisuuksiin. Tietoturvan peruskäsitteitä ovat käytettävyys ja saatavuus, luottamuksellisuus, eheys, kiistämättömyys, pääsynvalvonta sekä autentikointi ja tunnistaminen. [5.]

Tietoturvan perusperiaatteisiin kuuluvat tietoturvan osa-alueet, joita ovat fyysinen tietoturva, laitteisto- ja ohjelmistoturvallisuus, käyttöturvallisuus, henkilöstöturvallisuus, hallinnollinen sekä organisatorinen tietoturva, tietoliikenne- ja tietoaineistoturvallisuus [5]. Organisaatioympäristössä tietoturvaa tasapainotellaan muun muassa tietoturvan tehokkuuden, järjestelmän käytettävyyden, henkilöiden yksityisyyden sekä organisaation kustannuksien välillä [6]. Sopivan tasapainon löytäminen on hankalaa, koska se on tilannekohtaista. Tasapainottelu on myös tarpeen, sillä täydellistä järjestelmää ei ole [7].

Tietoturvan kannalta vahingon torjunta on halvempaa kuin sen korjaaminen, sillä tietoturvalla pyritään suojelemaan arkaluontoisia tietoja. Toisto on turvallisuuden vihollinen, koska järjestelmällistä käyttäytymistä voidaan ennakoida. Tietoturva on Petteri Järvisen mukaan 20 % tekniikkaa ja 80 % psykologiaa. Tämän vuoksi tiedolla on taipumus levitä ja todellista tietoturvaa ei voi kaupasta ostaa. Ainoa täysin turvallinen järjestelmä on sellainen, jossa ei ole yhtään käyttäjää. [5.]

3.1 Peruskäsitteet

Käytettävyydellä pyritään siihen, että tietoturva on niin sanotusti läpinäkyvää eli käyttäjä ei huomaa tietoturvan lisäämiä toimintoja. Käyttäjästä ei saisi koskaan tuntua siltä, että tietoturva hidastaa hänen toimintaansa. Hyvällä käytettävyydellä voidaan ehkäistä tietoturva-aukkoja, koska vaikeakäyttöisillä järjestelmillä ja ohjelmistoilla on suurempi riski altistua käyttäjän aiheuttamille tietoturva-aukoille. Esimerkiksi käyttäjä voi tietämättään sotkea järjestelmän asetuksia

Hyvä esimerkki tietoturvajärjestelmän käytettävyydestä on käyttäjätunnus ja salasana. Käyttäjätunnuksen sekä salasanan kysyminen sisäänkirjautumisen yhteydessä on hyväksyttävää, koska siihen ei kulu paljoa aikaa. Toisaalta, jos tunnuksia kysytään jatkuvasti tai lyhyen ajan välein, käyttäjät ärsyyntyvät, vaikka tietoturva teoriassa parantuukin. Käytettävyyden kannalta kasvavaksi ongelmaksi on muodostunut salasanojen muistaminen. Salasanoista kehotetaan tekemään pitkiä ja monimutkaisia, mutta samalla muistutetaan, että niitä ei saisi missään tapauksessa kirjoittaa muistiin [8]. Toisin sanoen käytettävyyttä hankaloittaa epäsuorasti käyttäjän käyttämien salasanojen määrä.

Saatavuudella tarkoitetaan, että tietoon päästään käsiksi aina, kun sitä halutaan käsitellä. Saatavuutta voidaan parantaa hyvällä suunnittelulla, varasuunnitelmilla ja epäsuorasti myös varmuuskopioinnilla. Esimerkiksi miten toimitaan, jos tietoa sisältävä palvelin kaatuu? Tällaisessa tilanteessa varmuuskopiointi toimii eräänlaisena varasuunnitelmana. Varmuuskopiointi on tärkein keino saatavuuden varmistamiseen [5]. Sen avulla voidaan varautua ääritilanteisiin, joissa tieto menetetään palautuskelvottomaksi. Tämän takia säännöllinen varmuuskopiointi on suositeltavaa myös simulaatioympäristöjen ulkopuolella.

Nykyään saatavuuden suunnittelua sekä toteutusta hankaloittaa käyttäjien halu etätyöskennellä useassa paikassa usealla eri laitealustalla. Organisaatio ei pysty ennakoimaan etätyöskentelijän tietoturvan laatua. Mobiililaitteita unohdetaan esimerkiksi julkisiin liikennevälineisiin matkustamisen aikana, jolloin laitteen tietoturva on uhattuna [5]. Etätyöskentelijän mobiililaite on myös voinut saastua kotikäytössä. Mobiililaitteisiin kohdistuu myös enemmän fyysistä rasitusta, kun niitä siirretään paikasta toiseen ja käytetään lentokoneen ja junan kaltaisissa ympäristöissä [5].

Tietoturvassa luottamuksellisuudella tarkoitetaan sitä, että vain oikeutetut henkilöt pääsevät käsiksi tietoon. Luottamuksellisuutta voidaan parantaa muun muassa salauksella sekä henkilöiden todentamisella. Henkilöiden todentamisella tarkoitetaan varmistumista siitä, että henkilö on juuri se, mitä hän väittää olevansa. Digitaalisessa todennuksessa hyödynnetään sähköisiä todistuksia eli sertifikaatteja. [9.]

Eheydellä tarkoitetaan sitä, että tieto pysyy siinä muodossa, jossa se on tallennettu. Esimerkiksi viestiin ei saa tulla matkalla muutoksia, vaan sen oltava sama sekä lähettäjällä että vastaanottajalla. Eheys voi särkyä myös tahattomasti esimerkiksi levylle tulleen vika-alueen tai tiedonsiirrossa tapahtuneen virheen vuoksi. Virheitä voi sattua myös käsittelyn aikana, esimerkiksi tietoa siirrettäessä ohjelmien välillä. Eheyden varmistamiseen käytetään muun muassa lokeja sekä tarkistussummia. [5.]

Autentikoinnilla eli todentamisella tarkoitetaan henkilön tunnistamista. Tunnistamiseen voidaan käyttää useita eri menetelmiä, kuten esimerkiksi käyttäjätunnusta ja salasanaa, varmenteita, henkilökortteja sekä videotallenteita. Tunnistus videotallenteiden avulla perustuu henkilön yksillöllisiin ominaisuuksiin, kuten esimerkiksi ulkonäköön tai ääneen. [5.]

Pääsynvalvonta huolehtii siitä, että vain autentikoidut henkilöt pääsevät käsiksi järjestelmään tai sen tietoihin. Pääsynvalvonnasta vastaavat käyttöjärjestelmä sekä sovellus. Pääsynvalvontaan liittyy myös käsite käytön seuranta. Järjestelmä voi esimerkiksi pitää lokitiedostoja käyttäjistä, jotka ovat avanneet tai muokanneet tiedostoja. Näitä tiedostoja voidaan käyttää hyväksi muun muassa tietomurtojen selvittämisessä. [5.]

Kiistämättömyydellä pyritään siihen, että käyttäjät eivät voi kiistää tekemisiään. Kiistämättömyydestä huolehtimen on erityisen tärkeää sähköisessä kaupankäynnissä, jossa osto- tai myyntitapahtuman vaiheet pitää voida sitovasti todistaa [5]. Kiistämättömyys voidaan saavuttaa luotettavilla aikaleimoilla sekä soveltamalla aiempia periaatteita eheydestä ja autentikoinnista [5]. Esimerkiksi myös käyttäjätunnus sekä salasana ovat osa kiistämättömyyttä, silloin kun jokaisella käyttäjällä on henkilökohtainen käyttäjätunnus.

3.2 Osa-alueet

Fyysinen tietoturva ja laitteistoturvallisuus pyrkivät ottamaan huomioon ulkoiset riskit. Ulkoisia riskejä ovat esimerkiksi tulipalot, vesivahingot, sähkökatkot sekä vihamieliset henkilöt. Fyysinen tietoturva keskittyy näiden riskien minimoimiseen ja ehkäisemiseen. Esimerkiksi järjestelmän sijainnilla ja sijaintiin liittyvillä tekijöillä, kuten palo-ovilla, voidaan vaikuttaa ulkoisiin riskeihin huomattavasti. Fyysinen tietoturva vaikuttaa epäsuorasti myös laitteistoturvallisuuteen, sillä laite, joka sijaitsee turvallisessa ympäristössä, ei ole niin altis ympäristön aiheuttamille haittatekijöille. Laitteistoturvallisuudella pyritään varautumaan esimerkiksi sähkökatkoihin ja ottamaan huomioon laitteisiin liittyvät asiat. Näitä asioita ovat esimerkiksi laitteen elinikä ja laatu. Hyvälaatuisella laitteella on pienempi riski mennä rikki kuin huonolaatuisella. Tämä on oleellinen asia silloin, kun laite sisältää tärkeää tietoa tai laitteita ei ole tarkoitus uusia säännöllisin väliajoin.

Ohjelmistoturvallisuus pyrkii kartoittamaan ohjelmistoon liittyvät riskit. Näitä riskejä ovat esimerkiksi koodin eheys, bugit sekä luvattomat käyttäjät. Selkeä koodi voi parantaa ohjelmiston tietoturvallisuutta, sillä selkeämpää koodia on helpompi debugata ja muokata. Ohjelmistoturvallisuuteen liittyvät myös käsitteet lisenssien hallinta ja sovellusten rekisteröinti. [5.]

Henkilöstö- ja käyttöturvallisuuden tarkoitus on minimoida käyttäjien aiheuttamia riskejä [5]. Näitä riskejä voivat olla esimerkiksi virukset ja haittaohjelmat sekä vääränlainen käyttö. Vääränlaisella käytöllä tarkoitetaan muun muassa virheellistä tapaa sammuttaa tietokone tai muuta toimintaa, joka voi vaarantaa järjestelmän sisältävän tiedon. Henkilöstö- ja käyttöturvallisuutta pyritään parantamaan tietoturvatietoisuudella [5]. Tietoturvatietoisuutta voidaan lisätä säännöllisillä henkilöstön koulutuksilla sekä informaatiotilaisuuksilla. Henkilöstöturvallisuuteen liittyy myös työntekijöiden taustojen tarkistaminen, salassapitosopimukset sekä työntekijöiden perehdyttäminen työtehtäviin.

Tietoliikenne- ja tietoaineistoturvallisuus pyrkii minimoimaan ja ehkäisemään tiedonsiirron sekä tiedonkäsittelyn aikana tapahtuvia riskejä. Riskeihin sisältyvät muun muassa luvattomat käyttäjät, salakuuntelu, virheellinen käyttö sekä fyysisen tallennusjärjestelmän rikkoutuminen tai hukkuminen. Tietoliikenneturvallisuuden päämääränä on jatkuvuuden turvaaminen, eheyden varmistaminen sekä siirrettävän tiedon salaaminen. [5.]

Hallinnollinen ja organisatorinen tietoturva keskittyy yritysten ja organisaatioiden sisäiseen tietoturvaan ja tietoturvastrategioihin. Myös tietoturvaan liittyvät linjaukset ja vastuut ovat osa hallinnollista tietoturvaa [5]. Tämän alueen riskejä ovat esimerkiksi irtisanotut tai vihamieliset työntekijät ja heidän käyttäjätunnuksensa sekä korvaamattomat henkilöt. Henkilöä, jolle ei ole määritelty varahenkilöä, kutsutaan tietoturvassa korvaamattomaksi henkilöksi. Esimerkiksi yritykselle voi aiheutua taloudellista tappiota kyseisen henkilön sairastuessa. Riskeiltä voidaan suojautua laatimalla tietoturvapolitiikka ja tietoturvastrategia sekä järjestämällä säännöllisiä koulutuksia. Tietoturvapolitiikan ja -strategian ylläpito on tärkeää.

3.3 Tietoturvamittarit ja riskianalyysin menetelmät

Tietoturvaa on hyvin hankala mitata, koska se on abstrakti käsite. Tämän takia mittaamisesta saatuja tuloksia tulisi tarkastella ja soveltaa tilannekohtaisesti. Tietoturvan mittarit eivät ole verrattavissa esimerkiksi lämpömittareihin, jotka antavat konkreettisia arvoja, koska tietoturvamittarit ja niiden tulokset toimivat enemmänkin indikaattoreina. Indikaattoreina voivat toimia esimerkiksi haastattelut, tilannekuvat, salauksen vahvuuden luokittelu sekä erilaiset auditoinnit. [7.]

Tietoturvamittareiden kehittämisessä törmätään useisiin haasteisiin. Haasteina ovat muun muassa epävarmuus, sillä kehittäjien on vaikea arvioida tietyn tilanteen todennäköisyyttä. Tilannetta tarkkaillessa tarkkailijat eivät voi olla täysin varmoja siitä, että käyttäjät toimivat tarkkailuhetkellä niin kuin he käyttäytyisivät normaalisti. Järjestelmien monimutkaisuus aiheuttaa haasteita, koska kehittäjien pitäisi pystyä ottamaan kaikki mahdolliset tilanteet huomioon, jotta tietoturva voitaisiin taata. Riskitekijänä toimii useasti myös toinen henkilö, joka voi hyödyntää strategisia menetelmiä murtautuakseen järjestelmään. Riskit voivat myös vaihdella ajan myötä. [10.]

Tietoturvamittareita on kritisoitu siitä, että ne yksinkertaistavat monimutkaisia sekä käyttäjiin että tekniikkaan kohdistuvia tilanteita tai järjestelmiä, jotta tulokset voitaisiin esittää vertailukelpoisina [10]. Mittareilla ei myöskään pystytä huomioimaan tuuria tai järjestelmään murtautuvan henkilön motivaatiota. Toisaalta tietoturvan tehokkuutta olisi vielä vaikeampi kartoittaa ilman tietoturvamittareita. Tämän takia tietoturvamittareita ja tietoturvan indikaattoreita sekä riskianalyysimenetelmiä käytetään ja kehitetään. [7.]

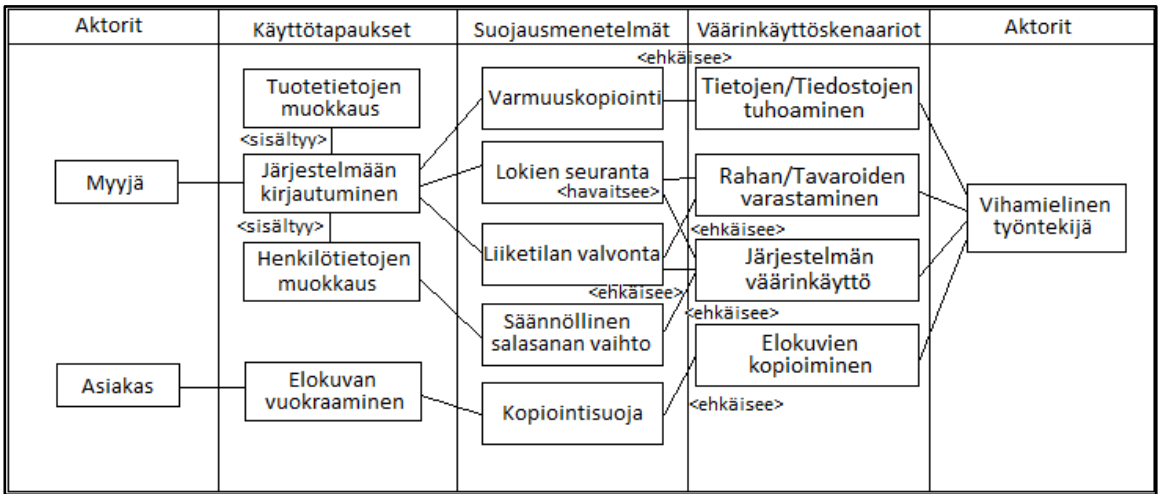
Tietoturvakartoitukseen käytettävät riskianalyysimenetelmät voidaan jakaa neljään päämenetelmään: Onnettomuuksien mallintaminen, seurausanalyysit, tarkistuslistat sekä vaarojen tunnistus. Onnettomuuksien mallintamiseen käytetään yleensä syy-seuraus-kaavioita, ja seurausanalyysit koostuvat usein teollisuuden häiriöiden vaikutuksista. Näitä häiriöitä ovat esimerkiksi vuodot, päästöt sekä räjähdykset. [11.]

Tarkistuslistat muodostetaan ennalta tehdyn riskikartan pohjalta, tai tarkistuslistana voidaan käyttää standardoituja tarkistuslistoja. Listan tulisi kuitenkin olla toimialakohtainen, sillä kaikilla aloilla ei ole samoja riskitekijöitä sekä myös aloihin liittyvät riskit vaihtelevat [11]. Tarkistuslistamenetelmien suurimpana heikkoutena on niiden pinnallisuus. Kysymyksiin vastataan yleensä kyllä tai ei, jonka vuoksi harmaalla alueella olevat vastaukset jäävät pimentoon. Tämän vuoksi tarkistuslistoja tulisi käyttää organisaation nykytilanteen kartoittamiseen jonkin toisen menetelmän yhteydessä. Tällöin tarkistuslistan vastaukset kiinnittäisivät huomiota ongelma-alueisiin, joiden tarkempaan kartoittamiseen käytetään syvällisempää menetelmää. Kuvassa 1 on esimerkki riskikartasta ja kuvassa 2 nähdään esimerkki tarkistuslistasta.

Kuva 1. Esimerkki organisaation riskikartasta.

Kuva 2. Esimerkkikuva tarkistuslistasta.

Vaarojen tunnistusmenetelmät sisältävät eniten asiakokonaisuuksia. Vaaroja voidaan tunnistaa muun muassa analysoimalla toimintovirheitä, työtapoja, vaarallisia tilanteita sekä mahdollisia ongelmia [11]. Toimintovirheiden ja työtapojen analysointia voidaan tehdä keskusteluilla sekä seuraamalla henkilöstön toimintaa. Vaarallisia tilanteita ja mahdollisia ongelmia voidaan analysoida ja havainnollistaa esimerkiksi skenaariokuvien avulla. Kuvassa 3 on esimerkki skenaariokuvasta.



Kuva 3. Videovuokraamon väärinkäyttötapausesimerkki.

SWOT (Strengths, Weaknesses, Opportunities, Threats) -analyysi on hyödyllinen ja yksinkertainen työkalu, jota käytetään yleensä jonkun toiminnan tai projektin suunnitteluun ja kehittämiseen. SWOT-analyysia voidaan käyttää myös organisaation riskianalyyseissä, ja se voi olla joko nelikenttäinen tai kahdeksankenttäinen. Nelikenttäisessä analyysissä taulukon ylhäällä oleviin kenttiin kirjataan kohteen sisäiset vahvuudet sekä heikkoudet. Alhaalla oleviin kenttiin kirjataan aiheen ulkoiset mahdollisuudet ja uhat. Kuvassa 4 on esimerkki nelikenttäisestä SWOT-analyysistä. Kuvassa 5 nähdään esimerkki kahdeksankenttäisestä SWOT-analyysistä, jossa alkuperäisistä kentistä on luotu yhdistelemällä neljä uutta kenttää.

Sisäinen	Sisäinen
Vahvuudet (V)	Heikkoudet (H)
Ulkoinen	Ulkoinen
Mahdollisuudet (M)	Uhat (U)

Kuva 4. Nelikenttäisen SWOT-analyysin pohja.

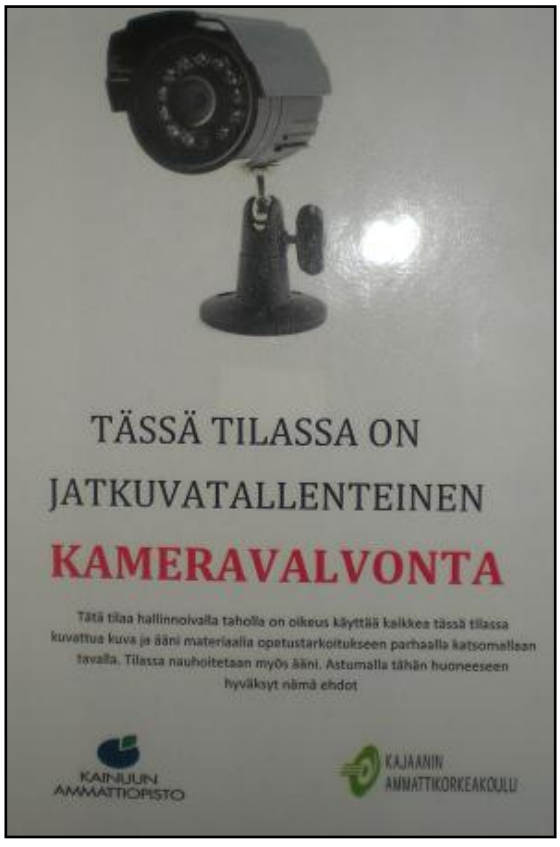
Analysoitava aihe	Vahvuudet (V) - esimerkki 1 - esimerkki 2 - esimerkki 3	Heikkoudet (H) - esimerkki 1 - esimerkki 2 - esimerkki 3
Mahdollisuudet (M) - esimerkki 1 - esimerkki 2 - esimerkki 3	Hyökkäysstrategia (V+M) Vahvuuksien hyödyntäminen mahdollisuuksien maksimoimiseksi	Hyökkäysstrategian kehitys (H+M) Heikkouksien torjuminen mahdollisuuksien kautta
Uhat (U) - esimerkki 1 - esimerkki 2 - esimerkki 3	Puolustusstrategia (V+U) Vahvuuksien hyödyntäminen uhkien minimoimiseksi	Puolustusstrategian kehitys (H+T) Heikkouksien ja uhkien torjuminen

Kuva 5. Kahdeksankenttäinen SWOT-analyysiesimerkki.

4 KAJAANIN AMMATTIKORKEAKOULUN JA KAINUUN AMMATTIOPISTON SIMULAATIO-OPPIMISYMPÄRISTÖ

Kajaanin ammattikorkeakoulu ja Kainuun ammattiopisto ovat hankkineet yhteistyöllä simulaatiojärjestelmän parantaakseen sosiaali- ja terveysalojen opetusta. Simulaatio-oppimisympäristöä käyttää maanantaisin ja tiistaisin Kainuun ammattiopisto, ja Kajaanin ammattikorkeakoulu käyttää järjestelmää torstaisin ja perjantaisin. Opetuslaitokset vuorottelevat keskiviikkoja viikoittain, ja ne ylläpitävät järjestelmää yhteistyöllä. [12.]

Kajaanin ammattikorkeakoulun simulaatio-oppimisympäristö sijaitsee Kajaanin ammattikorkeakoulun Taito 2 -rakennuksen alimmassa kerroksessa (TA2-0L118). Kuvassa 6 nähdään simulaatio-oppimisympäristön ovessa oleva ilmoitus opetustarkoitukseen käytettävästä kameravalvonnasta.



Kuva 6. Ilmoitus kameravalvonnasta.

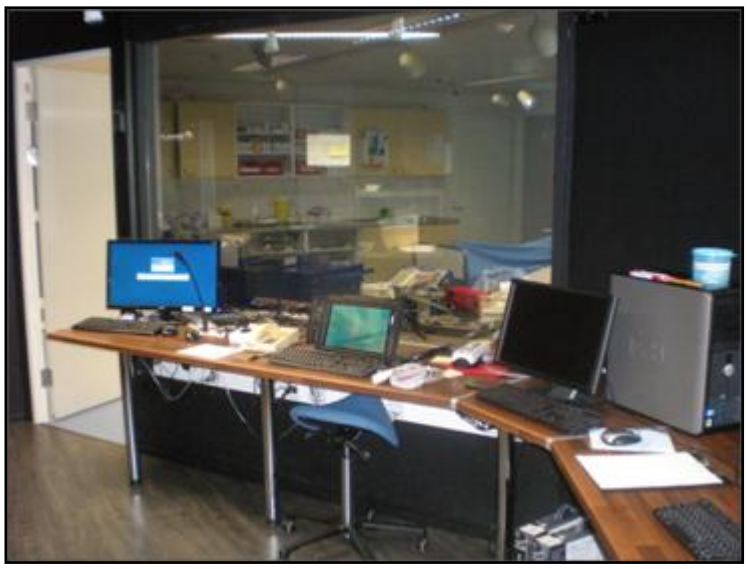
Simulaatiojärjestelmä on hajautettu neljän huoneen välille: debriefing, valvomo, simuloitu kotiympäristö ja simuloitu sairaalaympäristö. Debriefing-tilassa ohjaajat käyvät läpi harjoiteltua skenaariota osallistujien kanssa tallenteiden avulla [2]. Kuvassa 7 on debriefing-tila, ja kuvassa 8 nähdään debriefing-tilan näkymä skenaarion aikana.

Kuva 7. Debriefing-tila.

Kuva 8. Debriefing-tilan näkymä.

Valvomoon tarvitaan kaksi järjestelmän tuntevaa henkilöä käyttämään potilassimulaattoria, vitalmonitoria ja kameroita. Henkilöt voivat myös toimia potilaan äänenä sekä antaa yleisellä äänellä osallistujille arvoja, joita he eivät muuten pysty huomaamaan. Esimerkiksi he voivat sanoa "potilaan kädet ovat kylmät" [2]. Valvomosta nähdään molempiin simulaatiohuoneisiin, mutta simulaatiohuoneista ei voi nähdä valvomoon. Kuvassa 9 on näkymä valvomosta kotiympäristöön suunnattuna ja kuvassa 10 sairaalaympäristöön suunnattuna.

Kuva 9. Valvomo ja kotiympäristö.



Kuva 10. Valvomo ja sairaalaympäristö.

Simuloidut ympäristöt ovat keskenään samantapaisia eikä niitä käytetä samanaikaisesti [12]. Molemmissa huoneissa on kaksi paikallaan pysyvää kameraa sekä yksi kamera, jota voidaan liikuttaa järjestelmän avulla. Kaikissa kameroissa on myös pimeänäkö [13]. Skenaariosta riippuen voidaan käyttää joko aikuisnukkea, lapsinukkea tai molempia [13]. Nuket ovat yhteydessä järjestelmään, ja järjestelmän avulla niiden arvoja voidaan muuttaa. Esimerkiksi nuken pulssia voidaan kohottaa [2]. Kuvassa 11 nähdään nuket sairaalaympäristössä, kuvassa 12 on sairaalaympäristön tarvikekaapit ja kuvassa 13 nähdään kotiympäristö.

Kuva 11. Nuket sairaalaympäristössä.

Kuva 12. Sairaalaympäristö.

Kuva 13. Kotiympäristö.

Simulaatioskenaariot aloitetaan noin 15 minuutin briefingillä, jonka aikana ohjaajat kertovat osallistujille tilanteen, potilastiedot sekä muut oleelliset tiedot, jotta skenaario voidaan suorittaa. Briefingin jälkeen aloitetaan toimintaosuus, jonka aikana osallistujat reagoivat simuloituun tilanteeseen ja toimivat noin 10–15 minuuttia. Toiminnan jälkeen siirrytään debriefingtilaan, jossa toimintaosuutta analysoidaan yhdessä kaikkien osallistujien kanssa. Debriefingtilassa käytävät keskustelut sekä tilanteen analysointi kestävät yleensä 30–45 minuuttia. Oppiminen tapahtuu vasta keskusteluvaiheessa, koska osallistujat huomaavat, mitä he olisivat voineet tehdä toisin ja miksi. Keskustelun aikana ohjaajat pyrkivät kitkemään osallistujilta vääränlaiset ajattelumallit, jotka johtivat virheisiin. [2.]

5 SIMULAATIO-OPPIMISYMPÄRISTÖN TIETOTURVAKARTOITUS

Opetuslaitokset huomasivat tarpeen tietoturvakartoitukselle, koska simulaatioympäristö on suuri projekti, joka sisältää tietotekniikkaa sekä tallenteita osallistujista.

5.1 Taustaa

Simulaatio-oppimisympäristön tietoturvakartoittamiseen on käytetty henkilöiden haastattelumenetelmää, joka pohjautui tarkistuslistan tapaisiin haastattelukysymyksiin. Haastattelukysymysten tarkoitus oli enemmänkin ohjata keskustelua oikeaan suuntaan kuin saada suoria vastauksia kysymyksiin. Käytetyt haastattelukysymykset ovat liitteessä 1. Tietoturvakartoituksessa käytettiin myös sovellettua toimitapatutkimusta. Menetelmät toteutettiin keskustelemalla simulaatio-oppimisympäristön keskeisimpien henkilöiden kanssa ja osallistumalla opetustilanteeseen katsojana. Keskustelujen ja havaintojen pohjalta on laadittu riskitaulukoita, joissa arvioidaan riskien todennäköisyyttä, suuruutta ja sitä, miten riskeihin voitaisiin varautua. On tehty myös väärinkäyttöskenaariokuvia, joiden tarkoitus on havainnollistaa mahdollisia väärinkäyttötilanteita.

Tietoturvakartoitukseen valittiin kyseiset menetelmät, koska simulaatio-oppimisympäristöön perehdyttäessä huomattiin, että todennäköisimmät riskit tulevat käyttäjien kautta. Menetelmät myös sopivat simulaatio-oppimisympäristön tietoturvakartoituksen tekemiseen hyvin, sillä menetelmät eivät vaikuttaneet henkilökunnan rutiiniin tai simulaatio-oppimisympäristöön. Esimerkiksi opetustilanteita ei tarvinnut perua riskianalyysin ajaksi ja haastateltavien henkilöiden kanssa oli helppo sopia aika haastattelulle. Haastatteluun oli tarkoitus ottaa henkilöitä, jotka päättävät simulaatio-oppimisympäristöön liittyvistä asioista, tuntevat järjestelmän ja ympäristön sekä käyttävät ympäristöä säännöllisesti. Valitut henkilöt vastasivat asetettua tavoitetta.

5.2 Riskianalyysi

Riskienkartoitustaulukot ovat toteutettu yhdistelemällä tietoja simulaatio-oppimisympäristössä tehdyistä havainnoista, haastatteluista sekä havainnoista, joita tehtiin osallistumalla opetustilanteeseen. Taulukot on luokiteltu kategorioihin, ja niihin on otettu simulaatioympäristön keskeisimmät riskit. Taulukon tuloksia on myös kuvattu tarkemmin. Riskien analysoimiseen on käytetty asteikkoa yhdestä viiteen, jossa luku yksi tarkoittaa pienintä ja viitonen suurinta. Riskin todennäköisyys on kerrottu riskin vahingon suuruudella, jotta riskit voidaan luokitella prioriteettijärjestykseen. Prioriteetin suuruuteen vaikuttaa myös tilannekohtaisuus. Esimerkiksi riskillä, jolla on suuri todennäköisyys, mutta se aiheuttaa pientä vahinkoa, voi olla suurempi prioriteetti kuin riskillä, joka on harvinainen, mutta aiheuttaa suurta vahinkoa. Tilannekohtaisuus tulee huomioida riskin tapahtuessa tai silloin, kun todennäköisyys riskille on erittäin suuri.

Taulukosta 1 nähdään simulaatio-oppimisympäristöön vaikuttavat ulkoiset ympäristöriskit. Tulipalo ja vesivahinko eivät ole simulaatioympäristölle ja sen laitteille kovin todennäköinen uhka. Tulipalon tulisi syttyä järjestelmän sisällä suuren vahingon aikaansaamiseksi. Laitteet voivat syttyä tuleen ylikuumenemisen kautta, mutta todennäköisyys sille on erittäin pieni. Vesivahingon todennäköisyys ja sen aiheuttaman vahingon suuruus on myös pieni, sillä järjestelmän laitteet on keskitetty valvomoon. Valvomo on omana huoneenaan, ja suurin osa laitteista sijaitsee pöydillä sekä kaapeissa. On siis erittäin epätodennäköisestä, että vesivahinko aiheuttaisi vahinkoa laitteille. Vesivahingoksi voidaan myös luokitella juoman kaatuminen näppäimistön, hiiren tai muun laitteen päälle, mutta laitteistoa käyttävä henkilöstö ei ruokaile simulaatioympäristössä. Sähkökatkojen todennäköisyys on suurempi kuin tulipalon tai vesivahingon. Sähkökatkon aiheuttama vahinko riippuu sähkökatkon pituudesta ja ajankohdasta. Esimerkiksi jos sähkökatko tapahtuu opetustilanteen aikana, aiheuttaa se suurta vahingoa. Todennäköisyys sille, että sähkökatko aiheuttaa vahinkoa järjestelmän laitteille, on pieni, ja yleensä tällaisissa tilanteissa vahinko rajoittuu tallentamattoman tiedon katoamiseen.

Taulukko 1. Ulkoiset ympäristöriskit.

Riskin nimi	Todennäköisyys	Vahingon suuruus	Ennaltaehkäisy	Prioriteetti
Tulipalo	1	2	Sammutuspeitteet, Palo-ovet	2
Vesivahinko	1	1	Laitteiden sijoitus	1
Sähkökatko	2	3	Varasuunnitelmat tilanteen sattuessa	6

Taulukosta 2 nähdään ulkopuolisiin henkilöihin liittyviä riskejä. Ulkopuolisen murtautuminen simulaatioympäristön järjestelmään ei ole todennäköistä, sillä järjestelmä ei sisällä arkaluontoista tietoa tai tietoa, josta pystyisi saamaan suurta taloudellista voittoa. Videotiedostojen luvaton käyttö vahingoittaa lähinnä videossa näkyvien henkilöiden yksityisyyttä sekä organisaation imagoa. Järjestelmä ei ole samassa verkossa Kajaanin ammattikorkeakoulun tai Kainuun ammattiopiston kanssa, joten järjestelmän kautta ei voida vaikuttaa organisaatioiden muihin asioihin.

Ulkopuolisen murtautuminen fyysisesti simulaatio-oppimisympäristöön on todennäköisintä silloin, kun tietoturva-aukko johtuu huolimattomuudesta. Esimerkiksi henkilökunnalta voi jäädä ovet lukitsematta tai henkilökunta ei kiinnitä tarpeeksi huomiota ympäristön lähellä liikkuviin henkilöihin. Ympäristö sijaitsee rakennuksen ulko-oven lähellä, ja ulko-oven eteen pääsee helposti autolla. Murtautujan on siis helppo päästä kohteeseensa nopeasti. Ulko-oven eteen on suunnattu tallentava valvontakamera, joka ehkäisee murtautumistilanteita. Simulaatioympäristö ei kuitenkaan ole todennäköinen kohde murtautumiselle, sillä samassa rakennuksessa sijaitsee esimerkiksi luokkahuoneita, joissa pidetään tietotekniikkakoulutusta. Murtautumisesta aiheutuvat vahingot riippuvat murtautujan tekemisistä. Esimerkiksi varkaudet sekä laitteiden rikkominen aiheuttavat taloudellista tappiota, mutta järjestelmän tiedostojen luvaton avaaminen vahingoittaa tallenteessa olevien henkilöiden yksityisyyttä.

Taulukko 2. Ulkoiset henkilöstöriskit.

Riskin nimi	Todennäköisyys	Vahingon suuruus	Ennaltaehkäisy	Prioriteetti
Ulkopuolinen murtatuu järjestelmään	1	2	Ajantasalla olevat tietoturvaohjelmat.	2
Ulkopuolinen pääsee fyysisesti paikan päälle tekemään vahinkoa	2	4	Huolellisuus, murtautumisen hankaloittaminen	8
Varkaudet	1	5	Varastamisen hankaloittaminen, huolellisuus	5

Taulukossa 3 on huomioitu sisäisiä henkilöstöriskejä. Olennaisia riskejä ovat tahallinen ja tahaton väärinkäyttö, ympäristössä tapahtuvien tilanteiden levittäminen ulkopuoliselle, varkaudet sekä uhkaava käytös. Tahallinen väärinkäyttö ei ole todennäköinen riski, sillä tämän hetkisellä henkilökunnalla ei ole motiivia siihen. Henkilökunta on myös kiinnostunut järjestelmän tietoturvasta, mikä viittaa siihen, että he haluavat järjestelmän olevan turvallinen. Tahallinen väärinkäyttö voi kuitenkin aiheuttaa vahinkoa organisaatiolle, jos väärinkäytöllä voidaan rikkoa laitteita. Tahallisella väärinkäytöllä voi myös aiheuttaa vahinkoa osallistujille. Esimerkiksi jos osallistujalle on sattunut nolo tilanne, ei hänestä tunnu mukavalta, jos ulkopuoliset saavat tietää tai nähdä tilanteen. Henkilökunta korostaa jokaisen skenaarion alussa, että simulaatioympäristössä tapahtuvat tilanteet kuuluvat vain niille, jotka ovat tilanteeseen osallistuneet.

Järjestelmän ohjelmiston tahaton väärinkäyttö ei ole todennäköinen riski, sillä henkilökunnan mielestä ohjelmisto on helppokäyttöinen ja vaatii vain kohtalaisen tietotekniikkaosaamisen. Järjestelmän laitteiden tahaton väärinkäyttö ei myöskään ole todennäköistä. Tietojen levittä-

minen ulkopuoliselle on todennäköinen riski, ja se loukkaa osallistujien yksityisyyttä. Henkilökuntaan kuuluva henkilö ei ole yhtä todennäköinen levittämään tietoa kuin osallistuja. Osallistuja voi esimerkiksi kantaa kaunaa toista osallistujaa kohtaan tai hän voi ajattelemattomuuden takia levittää tietoa eteenpäin. Esimerkiksi toiselle osallistujalle tapahtunutta noloa tilannetta voi toinen osallistuja pitää hauskana.

Riskinä ovat myös varkaudet. Koska skenaariot sijoittuvat simuloituun sairaalaympäristöön, varkauksien kohteena voivat olla esimerkiksi huumausaineiden käyttäjiä kiinnostavat tarvikkeet. Näiden tarvikkeiden menetys aiheuttaa hyvin pientä tai jopa huomaamatonta vahinkoa organisaatiolle.

Taulukko 3. Sisäiset henkilöstöriskit.

Riskin nimi	Todennäköisyys	Vahingon suuruus	Ennaltaehkäisy	Prioriteetti
Tahallinen väärinkäyttö	1	4	Henkilökunnan taustojen tarkistaminen	4
Tahaton väärinkäyttö	1	2	Koulutukset	2
Osallistuja käyttäytyy uhkaavasti	2	2	Tilanteeseen varautuminen	4
Osallistuja levittää tietoa eteenpäin	3	2	Asian korostaminen	6
Henkilökunta levittää tietoa eteenpäin	2	2	Asian korostaminen	4
Laitteistovarkaus	1	5	Varastamisen hankaloittaminen	5
Tiedosto- tai tarvikevarkaus	2	2	Käyttöoikeuksien rajoittaminen,	2

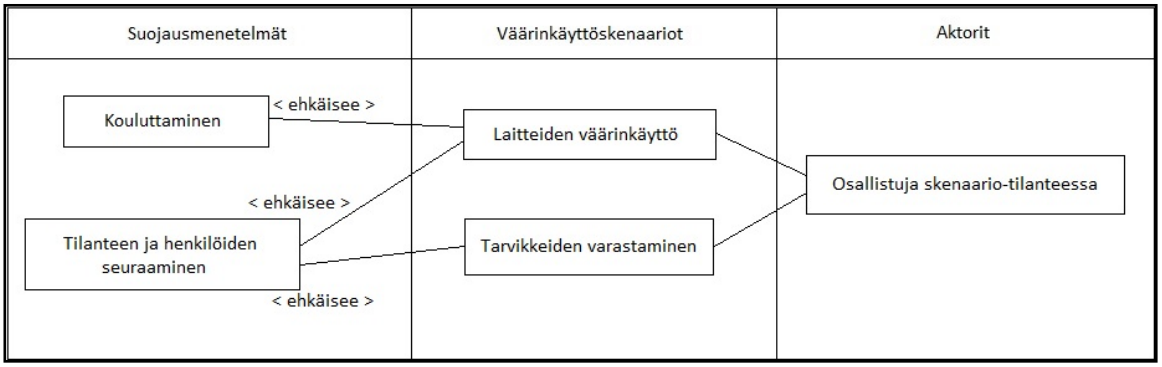
			tarkkaavaisuus	

Taulukkoon 4 on listattu laitteisto- ja ohjelmistoriskejä. Nämä riskit aiheuttavat suurta vahinkoa skenaariotilanteiden pitämiseen, sillä jos laitteet eivät toimi, ei skenaarioita pystytä pitämään. Laitteiden rikkoutuminen sekä ohjelmistovikojen ilmeneminen ajan myötä on todennäköistä. Tällä hetkellä laitteet ovat uusia, joten todennäköisyys on normaalia pienempi. Tämä ei kuitenkaan tarkoita sitä, etteikö riskiin kannattaisi varautua.

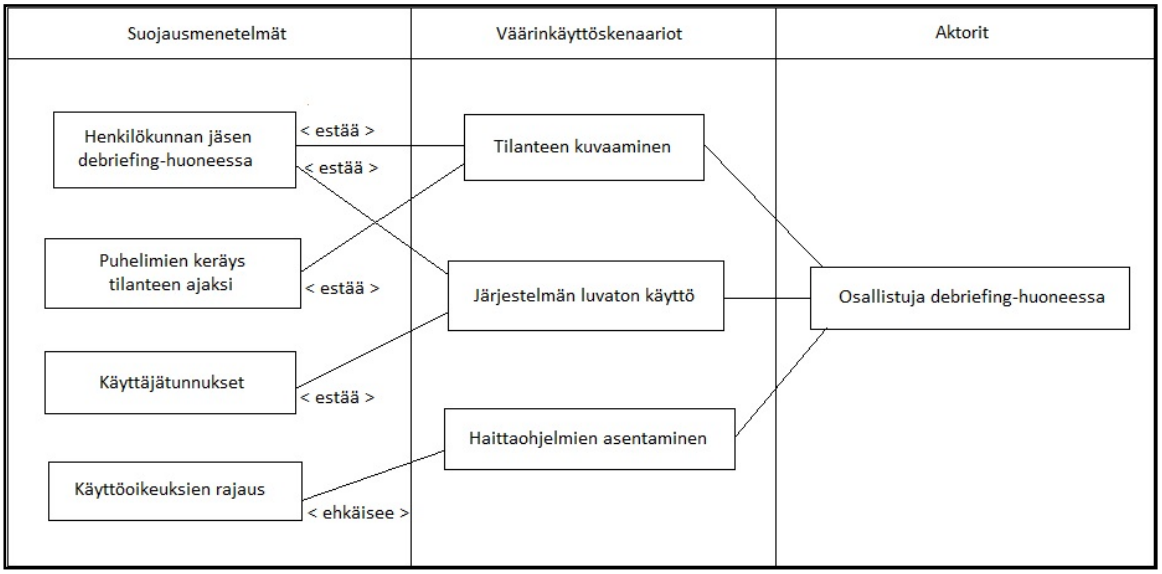
Taulukko 4. Laitteisto- ja ohjelmistoriskit.

Riskin nimi	Todennäköisyys	Vahingon suuruus	Ennaltaehkäisy	Prioriteetti
Rikkinäinen laite	1	5	Varalaitteet, varasuunnitelmat	5
Ohjelmistoviat	1	5	Asianmukainen käyttö	5
Tiedostojen/Tallenteiden menetys	1	1	Varmuuskopiointi	1

Kuvassa 14 nähdään muutamia mahdollisia simulaatiotilanteen aikana tapahtuvia väärinkäyttötapauksia ja menetelmiä, joiden avulla väärinkäyttötilanteet voidaan estää tai ehkäistä. Kuvassa 15 on kuvattu muutamia mahdollisia debriefing-tilan väärinkäyttötapauksia ja menetelmiä, joiden avulla väärinkäyttötilanteet voidaan estää tai ehkäistä.



Kuva 144. Väärinkäyttöskenaariokuva simulaatioympäristöstä.



Kuva 15. Väärinkäyttöskenaariokuva debriefing-tilasta.

5.3 Tulokset

Tietoturvakartoitus keskittyi enemmän simulaatio-oppimisympäristön käyttäjiin kuin sen tekniikkaan, koska riskienkartoitusanalyysien aikana havaittiin käyttäjien olevan suurempi riski simulaatio-oppimisympäristön tietoturvalle.

Tietoturvakartoituksen aikana ilmeni muutamia tietoturva-aukkoja, joihin annettiin kehitysehdotuksia. Kehitysehdotukset otettiin käyttöön nopeasti. Tietoturvakartoituksen aikana ha-

vaittuja tietoturva-aukkoja sekä niihin annettuja kehitysehdotuksia ei ole insinöörityöhön kirjattu asiakkaan pyynnöstä. Kehitysehdotukset annettiin erillisellä dokumentilla asiakkaalle.

Tietoturvakartoituksen tuloksena saatiin, että simulaatio-oppimisympäristön tietoturva on riittävällä tasolla sen käyttötarkoitusta kohden. Simulaatio-oppimisympäristön tietoturvaa on kuitenkin mahdollista parantaa. On kuitenkin hyvä pitää mielessä, että liian tiukka tietoturva heikentää järjestelmän käytettävyyttä. Jos simulaatio-oppimisympäristön käyttötarkoitus tai ympäristön sisältämät tiedot tulevaisuudessa muuttuvat, on uusi tietoturvakartoitus tarpeellinen.

Tietoturvakartoituksen tuloksia on myös mietitty tietoturvan peruskäsitteiden ja osa-alueiden kannalta. Simulaatio-oppimisympäristö pitää tallenteita saatavilla kahden viikon ajan, jonka aikana tiedostoja voidaan siirtää tai tallentaa muualle. Viikon jälkeen järjestelmä aloittaa tallentamisen ajanjakson ylittäneiden tallenteiden päälle. Järjestelmä tarjoaa myös mahdollisuuden tallenteiden siirtämiseen sekä uudelleenkatsomiseen, mutta simulaatio-oppimisympäristöä käyttävät henkilöt eivät ole nähneet tarvetta näille ominaisuuksille. Tämä parantaa esimerkiksi videotallenteiden eheyttä sekä tietoaineistoturvallisuutta. Simulaatio-oppimisympäristön laitteet ovat laadultaan hyviä. Näiden asioiden perusteella voidaan sanoa, että järjestelmän laitteistoturvallisuus ja saatavuus ovat hyvällä tasolla.

Järjestelmä toimii omassa verkossa, ja sen käyttämiseen vaaditaan käyttäjätunnus sekä salasana. Järjestelmän tietokoneet on suojattu virustorjunnalla sekä palomuurilla, eikä ympäristöön pääse ilman henkilökunnan avainta. Nämä asiat parantavat ympäristön luottamuksellisuutta sekä myös tietoliikenne- ja tietoaineistoturvallisuutta. Kiistämättömyyden ja autentikoinnin kannalta ympäristöä käyttäneet henkilöt voidaan tunnistaa tallenteiden avulla. Kiistämättömyyteen ja autentikointiin vaikuttavat myös esimerkiksi päivämäärät, joista voidaan päätellä, kenen vuoro on ollut käyttää järjestelmää.

Simulaatio-oppimisympäristön laitteet sekä ohjelmistot ovat helppokäyttöisiä käyttäjille, jotka ovat tottuneet käyttämään tietokoneita eri työtehtävissä. Järjestelmän käyttö voi kuitenkin osoittautua hankalaksi, jos käyttäjällä ei ole aikaisempaa kokemusta tietotekniikkalaitteiden käytöstä.

6 KEHITYSEHDOTUKSET

Tietoturvakartoituksen aikana ilmeni muutamia tietoturva-aukkoja, jotka liittyivät muun muassa työtapoihin, käytäntöihin sekä huolimattomuuteen. Tietoturvakartoituksen aikana esitettiin kehitysehdotuksia riskien ehkäisemiseksi ja niiden estämiseksi. Kyseiset kehitysehdotukset otettiin käyttöön erittäin nopeasti jo tämän insinöörityön aikana. Työssä havaittuja tietoturva-aukkoja tai niihin annettuja kehitysehdotuksia ei ole tässä insinöörityössä mainittu, insinöörityön luonteen vuoksi.

Simulaatio-oppimisympäristön tietoturvaa on mahdollista parantaa esimerkiksi käyttöjärjestelmän sekä tiedostojen salauksella, mutta tietoturvan läpinäkyvyys heikkenisi. Järjestelmä ei myöskään sisällä arkaluontoisia tai tärkeitä tietoja, joiden menetys aiheuttaisi taloudellista haittaa. Tämän takia käyttöjärjestelmän tai tiedostojen kryptaaminen ei käytännön tasolla parantaisi tällä hetkellä simulaatio-oppimisympäristön tietoturvaa ollenkaan.

Tietoturvan ylläpito on jatkuva prosessi, jonka vuoksi säännölliset koulutukset parantavat tietoturvan tasoa minimoimalla tahattomia väärinkäyttötapauksia. Koulutukset voivat keskittyä esimerkiksi uusien ohjelmistojen käyttökoulutukseen tai vanhan kertaukseen. Valvomossa olisi hyvä olla aina vähintään yksi henkilö, joka on käyttänyt järjestelmää säännöllisesti, jotta opetustilanteet sujuisivat mahdollisimman sujuvasti. Säännölliset salasanan vaihdot sekä yhteisistä käytännöistä kiinnipitäminen kuuluvat myös tietoturvan ylläpitoon.

Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston kannattaisi miettiä yhdessä varasuunnitelmia ongelmatilanteiden varalle. Varasuunnitelmana voisi olla esimerkiksi toimintasuunnitelma tilanteeseen, jossa järjestelmä ei lähde käyntiin tai järjestelmä lakkaa toimimasta opetustilanteen aikana. Opetustilanteiden sujuvuuden kannalta ympäristössä olisi hyvä olla muutamia erilaisia varalaitteita, kuten esimerkiksi mikrofoneja. Tällä ehkäistään mahdollisten ongelmatilanteiden syntymistä.

7 YHTEENVETO

Insinöörityön tavoitteena oli tehdä Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston yhteistyöllä hankkimalle simulaatio-oppimisympäristölle tietoturvakartoitus. Tietoturvakartoituksen tavoite oli löytää sekä ehkäistä ympäristön mahdollisia haavoittuvuuksia ja heikkouksia.

Työssä käsiteltiin simulaatio-opetuksen hyötyjä teoriapohjaiseen opetukseen verrattuna, jonka jälkeen tutustuttiin tietoturvaa koskevaan teoriaan, kuten tietoturvan peruskäsitteisiin, osa-alueisiin sekä riskianalyysimenetelmiin ja tietoturvamittareihin. Tämän jälkeen käsiteltiin Kajaanin ammattikorkeakoulun ja Kainuun ammattiopiston simulaatio-oppimisympäristöä yksityiskohtaisemmin ja tutustuttiin ympäristölle tehtävän tietoturvakartoituksen tarkoitukseen.

Työn aikana tehty tietoturvakartoitus oli tarpeellinen, ja sen avulla ehkäistiin mahdollisia haavoittuvuuksia, sillä tietoturvakartoituksen aikana havaittiin muutamia tietoturva-aukkoja sekä haavoittuvuuksia. Näihin haavoittuvuuksiin puututtiin nopeasti annettujen kehitysehdotusten avulla. Tietoturvakartoituksen lopputulos oli, että simulaatio-oppimisympäristön tietoturva on riittävä sen nykyiselle käyttötarkoitukselle, ja jos käyttötarkoitus muuttuu, on uusi tietoturvakartoitus tarpeellinen. Tulosten yhteydessä ilmoitettiin myös, että ympäristön tietoturvaa on mahdollista parantaa tulevaisuudessa, mutta parannukset voivat kuitenkin heikentää järjestelmän käytettävyyttä.

Opinnäytetyön tilaajalle annettiin yksityiskohtaisempia kehitysehdotuksia sekä riskikuvauksia erillisellä dokumentilla simulaatio-oppimisympäristön tietoturvaan liittyen. Tilaajalle annettiin myös erillisellä dokumentilla yksityiskohtaisempi riskianalyysi. Näiden dokumenttien tarkoitus oli parantaa ympäristön tietoturvaa aiheuttamatta uusia haavoittuvuuksia tämän insinöörityön kautta.

LÄHTEET

1 Järvinen, P.Yksityisyys - Turvaa digitaalinen kotirauhasi, 1. painos. Jyväskylä: WSOYpro Oy, 2010. 15 s. ISBN 951-846-36157-3

2 Seppänen, J. - Lehtori, Riskienkartoitus, 6.6.2012, [Haastattelu]

3 VAHTI, Tietoturvakouluttajan opas [PDF-dokumentti], <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061128Tietot/Vahti_11_06.pdf> (muokattu 28.11.2006)

4 Simulaatio-opetus ensihoidossa [PDF-dokumentti], <http://www.finnanest.fi/files/hallikainen_simulaatio.pdf> (Luettu 13.9.2012)

5 Järvinen, P. Tietoturva ja yksityisyys, 1. painos. Porvoo: Docendo Finland Oy, 2002. 22-28, 44, 79-80 s. ISBN 951-846-152-X

6 Savola, R – Principal Scientist at VTT, The future of information security – Technical and research perspective, 10.11.2012, [PowerPoint-esitys]

7 Savola, R. - Principal Scientist at VTT, Security metrics – How and where they can be used?, 6.11.2012, [Luento]

8 VAHTI, Peruskäyttäjän koulutusopas, [PowerPoint-esitys] <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061128Tietot/Peruskayttajan_Koulutusmateriaali_V6_2006-11-05.ppt> (muokattu 28.11.2006)

9 Järvinen, P. Salausmenetelmät, 1. painos. Porvoo: Docendo Finland Oy, 2003. 159 s. ISBN 951-846-183-X

10 Savola, R - Principal Scientist at VTT, Security metrics – How and where they can be used?, 10.11.2012, [PowerPoint-esitys]

11 Rantanen, R. Riskianalyysimenetelmiä [PDF-dokumentti], (Luettu 6.10.2012)

12 Juntunen, J. - Tuntiopettaja, Riskienkartoitus, 6.10.2012, [Haastattelu]

13 Romppanen, T. - Lehtori, Riskienkartoitus, 27.9.2012, [Haastattelu]

LIITTEET

LIITE 1 - Haastattelukysymykset

Kerro miten simulaatio-oppimisympäristön käyttö kulkee? Esimerkiksi alkutoimet, skenaario, lopputoimet.

Onko simulaatio-oppimisympäristön laitteiden käyttäjillä henkilökohtaiset käyttäjätunnukset ja salasanat, vai onko käytössä yleiset tunnukset (kaikille samat)? Onko tilanteessa eroa debriefing-tietokoneen ja valvomo-tietokoneen välillä?

Miten toimitaan kun simulaatioympäristöstä lähdetään pois (joko kesken kaiken tai tilaisuuden päätyttyä)? Jääkö laitteet päälle?

Miten toimitaan, jos järjestelmä ei toimi halutulla tavalla? Esimerkiksi puhe ei kuulu mikrofoneista tai nuken arvoja ei voida muokata? Toisin sanoen, onko mietitty varasuunnitelmia tällaisia tilanteita varten? Jos on, millaisia?

Katsotaanko tallenteita myöhempänä ajankohtana tai julkaistaanko niitä?

Onko tilaisuuteen osallistujilla mahdollisuutta jälkikäteen katsella häneen kohdistuva tallenne/skenaario uudelleen?

Siirretäänkö tallenteita pois simulaatio-oppimisympäristöstä? Esimerkiksi USB-tikulla etätyöskentelyä varten.

Kuinka monella henkilöllä on pääsy simulaatio-oppimisympäristön tiloihin?

Miten toimitaan tilanteissa, joissa jollekin henkilölle tapahtuu jotain noloa? Esimerkiksi intiimipaikka näkyy.

Onko käytössä mitään ”salassapitosopimusta”? Esimerkiksi painotetaan sitä, että simulaatio-oppimisympäristössä tehdyistä virheistä huudella kaupungilla.

Tehdäänkö tallenteista varmuuskopioita?

Onko järjestelmä mielestäsi helppokäyttöinen?

Tarvitseeko sinun huolehtia tallenteiden poistamisesta vai tapahtuuko se automaattisesti?

Kerätäänkö puhelimet pois tilaisuuden ajaksi? Kielletäänkö osallistujia kuvaamasta omaa materiaalia?